Advisory Alert

Alert Number: AAA20240315 **Date:** March 15, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
IBM	**High**	Denial of Service Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has issued security updates addressing multiple vulnerabilities that exist in Dell EMC VxRail Appliance. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell EMC VxRail Appliance 8.0.x versions prior to 8.0.210
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223129/dsa-2024-050-security-update-for-dell-vxrail-multiple-third-party-component-vulnerabilities-8-0-210

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38408, CVE-2023-44288, CVE-2023-44295, CVE-2023-32458, CVE-2022-3715, CVE-2023-0286, CVE-2022-4304, CVE-2023-0215)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure, Local Privilege Escalation, Use-After-Free. Dell advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerScale OneFS all versions Dell EMC AppSync versions 4.4.0.0, 4.5.0.0 and 4.6.0.0 including Service Pack releases
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000219932/dsa-2023-417-dell-powerscale-onefs-security-updates-for-multiple-security-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000218038/dsa-2023-331-dell-emc-appsync-security-update-for-dell-embedded-service-enabler-vulnerability https://www.dell.com/support/kbdoc/en-us/000212709/dsa-2023-136-dell-powerscale-onefs-security-updates-for-multiple-security-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42896, CVE-2023-4921, CVE-2023-38409, CVE-2023-45871, CVE-2024-1086, CVE-2024-26602)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Enterprise Linux. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Use-After-Free, Information Leak, Local Privilege Escalation and Buffer Overflow. Red Hat advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1332

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-25162, CVE-2021-46923, CVE-2021-46924, CVE-2021-46932, CVE-2021-46934, CVE-2021-47083, CVE-2022-48627, CVE-2023-28746, CVE-2023-5197, CVE-2023-52340, CVE-2023-52429, CVE-2023-52439, CVE-2023-52443, CVE-2023-52445, CVE-2023-52447, CVE-2023-52448, CVE-2023-52449, CVE-2023-52451, CVE-2023-52452, CVE-2023-52456, CVE-2023-52457, CVE-2023-52463, CVE-2023-52464, CVE-2023-52467, CVE-2023-52475, CVE-2023-52478, CVE-2023-52482, CVE-2023-52484, CVE-2023-52530, CVE-2023-52531, CVE-2023-52559, CVE-2023-6270, CVE-2023-6817, CVE-2024-0607, CVE-2024-1151, CVE-2024-23849, CVE-2024-23850, CVE-2024-23851, CVE-2024-26585, CVE-2024-26586, CVE-2024-26589, CVE-2024-26591, CVE-2024-26593, CVE-2024-26595, CVE-2024-26598, CVE-2024-26602, CVE-2024-26603, CVE-2024-26607, CVE-2024-26622)
Description	Suse has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to Out-of-Bounds Memory Access, Use-After-Free and NULL Pointer Dereference. Suse recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4 openSUSE Leap Micro 5.3, 5.4 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4, ESPOS 15 SP4, LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4, 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240900-1/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-52425)
Description	IBM has released security updates addressing a Denial of Service Vulnerability in IBM HTTP Server, which is used by IBM WebSphere Application Server. A remote attacker could exploit this vulnerability by sending a specially crafted request using an overly large token caused by improper system resource allocation in libexpat. IBM recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere Remote Server v9.0, v8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7142031

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.